Order Code RL30735

CRS Report for Congress
Received through the CRS Web

Cyberwarfare

Updated June 19, 2001

Steven A. Hildreth
Specialist in National Defense
Foreign Affairs, Defense, & Trade Division

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	6/19/2001	Report 6/19/2001

4. TITLE AND SUBTITLE
Cyberwarfare

5. FUNDING NUMBERS

6. AUTHOR(S)
Steven A. Hildreth

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Congressional Research Service The Library of Congress

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

Cyberwarfare raises issues of growing national interest and concern. Cyberwarfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same. Some major problems encountered with cyber attacks, in particular, are the difficulty in determining the origin and nature of the attack and in assessing the damage incurred. A number of nations are incorporating cyberwarfare as a new part of their military doctrine. Some that have discussed the subject more openly include the United Kingdom, France, Germany, Russia, and China. Many of these are developing views toward the use of cyberwarfare that differ from those of the United States, and in some cases might represent national security threats.

14. SUBJECT TERMS
IATAC Collection, cyberwarfare, war, cyberspace, cyberterrorist, eligible receiver, solar sunrise,

15. NUMBER OF PAGES
20

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Cyberwarfare

Summary

Cyberwarfare raises issues of growing national interest and concern. Cyberwarfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same. Some major problems encountered with cyber attacks, in particular, are the difficulty in determining the origin and nature of the attack and in assessing the damage incurred.

A number of nations are incorporating cyberwarfare as a new part of their military doctrine. Some that have discussed the subject more openly include the United Kingdom, France, Germany, Russia, and China. Many of these are developing views toward the use of cyberwarfare that differ from those of the United States, and in some cases might represent national security threats.

Cyberterrorism is also an issue of growing national interest. Many believe terrorists plan to disrupt the Internet or critical infrastructures such as transportation, communications, or banking and finance. It does seem clear that terrorists use the Internet to conduct the business of terrorism, but on closer inspection, however, it is not clear how or whether terrorists could use violence through the Internet to achieve political objectives.

Although the U.S. government is striving to consolidate responsibility for and focus more attention on cyberwarfare issues, it is not clear how successful those efforts will be. Congress may choose to examine critically the policies, organization, and legal framework that guides executive branch decisionmaking on issues of cyberwarfare.

Contents

Cyberwarfare

Introduction

Background

There is a war being waged in cyberspace[1] today – at least that's what many in government and the media would have us believe. Former Deputy Secretary of Defense John Hamre testified to Congress, for example, that "you can basically say we are at war." More recently, President Bush and Defense Secretary Rumsfeld both acknowledged that cyberwarfare is an emerging threat to U.S. national security.[2]

A couple of years ago, the Central Intelligence Agency (CIA) only mentioned Russia and China specifically as possible cyber threats. Today, U.S. officials indicate that more than 20 countries have various kinds of information operations (IO) directed against the United States. The CIA testified more recently that adversaries are incorporating cyberwarfare[3] as a new part of their military doctrine. A declassified

---

[1] ***Cyberspace*** is the total interconnectedness of human beings through computers and telecommunication without regard to physical geography. William Gibson is sometimes credited with inventing or popularizing the term by using it in his novel of 1984, *Neuromancer*. Cyberspace is often used as a metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse. Some programs, particularly computer games, are designed to create a special cyberspace, one that resembles physical reality in some ways but defies it in others. In its extreme form, called virtual reality, users are presented with visual, auditory, and even tactile feedback that makes cyberspace feel real. See, for instance, [http://aol.pcwebopedia.com/TERM/c/cyberspace.html].

[2] See, "Remarks by the President and Secretary of Defense Donald Rumsfeld Swearing-In Ceremony," The Oval Office, Office of the Press Secretary, Jan. 26, 2001; President Bush, "Remarks to Central Intelligence Agency Employees in Langley, Virginia," *Weekly Compilation of Presidential Documents*, Washington, DC, March 26, 2001; and "Secretary of Defense Donald Rumsfeld Interview on Fox News Sunday," Feb. 11, 2001, *News Transcript*, U.S. Department of Defense.

[3] A number of terms are used to describe the various aspects of defending and attacking information and computer networks, as well as denying an adversary's ability to do the same, or even dominating the information environment on the battlefield. These terms are more accurately defined later in the section on Terms & Definitions. Meanwhile, cyberwarfare in this report will be used broadly to refer to these various activities. More specifically, it can

(continued...)

Navy threat assessment identifies Russia, China, India, and Cuba as countries who have acknowledged policies of preparing for cyberwarfare and who are rapidly developing their capabilities. North Korea, Libya, Iran, Iraq, and Syria reportedly have some capability, and France, Japan, and Germany are active in this field.[4]

The media and others often also warn of cyberterrorists waiting for the right moment to bring down the U.S. power, transportation, or communications grids. For example, at a hearing of the Joint Economic Committee on cyberterrorism that included the CIA (Feb. 23, 2000), Sen. Bob Bennett said, "attacks on American defense and industrial facilities in cyberspace are as real and dangerous as any conventional threat to economic prosperity and national security."

But is all this really war or warfare? Computer systems at the Pentagon and other military sites get "attacked" thousands of times each year. But is it war if many or most of those attacks come from teenagers here in the United States, or even abroad? Does the military even *know* how many of those attacks it should genuinely be worried about? Is an attempt by a foreign nation to collect military secrets via the Internet or modem an act of war for which the United States is prepared to respond coercively? Should the United States respond in kind by waging war in cyberspace? What constitutes victory in cyberspace? Or is spying traditionally considered something else, something less than war? If another nation systematically attacks U.S. business networks to steal trade secrets in support of its own economic interests or to pass those secrets on to their own corporations for competitive advantage, is that warfare? Does the answer change if the attacking nation is a U.S. ally or friend?

So what is the appeal of cyberwarfare or information warfare? Why choose cyberwarfare over other forms of warfare or conflict? Many see that it provides a range of relatively anonymous, non-lethal options that can be applied at the speed of light and with relatively low risk of escalation to more direct forms of conflict. In one sense, it's a way for others to wage an asymmetrical conflict against the United States. The likelihood of getting caught, let alone incurring U.S. military might, may seem low compared to the possible benefits. The appeal of cyberwarfare to the United States could grow out of the larger U.S. trend over the past twenty years to minimize conflict casualties and maximize technological advantages while pursuing increasingly activist foreign and defense policy agendas.

Purpose

This report is designed to examine broad cyberwarfare issues and raise underlying questions. The report first summarizes some cases that illustrate real-world concerns many have with respect to cyberwarfare. It then discusses the current U.S. policy and organizational approaches to cyberwarfare. The report also examines

---

[3](...continued)
include computer or network penetration, denial-of-service attacks on computers and networks, equipment sabotage through cyberspace, sensor jamming, and even manipulating trusted information sources to condition or control an adversary's thinking.

[4]Navy Names Nations Posing Cyber Threats. *Defense Week.* Sept. 5, 2000, p. 1. The Office of Naval Intelligence prepared the report.

foreign perspectives, the issue of cyberterrorism, and some reported instances of cyberwarfare. An appendix on terms and definitions is included at the end of the report. This report's focus is on cyberwarfare activities sponsored by nation-states, but includes cyberterrorism that is aimed at achieving political objectives at the national level.

It is important to point out that a large number of other kinds of cyber attacks take place regularly, but they will not be addressed by this report. In fact, these types of attacks are likely more frequent than state-sponsored activities or cyberterrorism. These other attacks or intrusions also are unauthorized attempts to access computers, computer controlled systems, or networks. These activities can range from simply penetrating a system and examining it for the challenge, thrill, or interest, to entering a system for revenge, to steal information, cause embarrassment, extort money, or cause deliberate localized harm to computers or damage to a much larger infrastructure, such as a water supply or energy system. These cyber attacks might be referred to as hacking, cyber mischief, cyber hooliganism, personal or corporate theft, revenge, or espionage, or organized crime activities (foreign and domestic). The realm for their resolution may lie in law enforcement and judicial systems, and legislative remedy where necessary.

Obviously, Congress plays a key role in the formulation, funding, conduct, and oversight of U.S. national security. The interplay of Congress and the Executive Branch on cyberwarfare issues in recent years is touched on later.

Nature of the Challenge: Case Studies

Several examples help illustrate the complexity of cyberwarfare, as well as the concern that many have. They show the difficulty in identifying the source and purpose of the attack, in determining whether a coordinated attack is underway, in assessing what seems to work and what does not, and calculating the damages incurred. The cases summarized below help raise an important question: does cyberwar represent a fundamentally new form of 21st century warfare, for which the United States may or may not be prepared, or is it simply a new tool for traditional asymmetric conflict, for which this country also may or may not be prepared to manage?

Air Force Rome Lab (1994)

In March 1994, system administrators at Rome Lab in New York found their network under attack. The Air Force dispatched two teams to investigate further. The attacks were traced to an ISP (Internet Service Provider) first in New York, then in Seattle, Washington, where the Internet path dead-ended (the attackers used dial-up lines). There was subsequent monitoring at Rome Lab and two hacker handles or aliases were identified – Kuji and Datastream Cowboy. Informants were solicited and someone recognized a hacker from the United Kingdom; this hacker had bragged that he had broken into various U.S. military systems. The United States then contacted

Scotland Yard. Scotland Yard discovered the hacker was "phreaking"[5] through Columbia and Chile to New York, defrauding telephone companies and the New York ISP as a jumping off point to attack Rome Lab. The UK hacker was later observed targeting other sites such as NATO headquarters, Goddard Space Flight Center, and Wright-Patterson Air Force Base. At least eight countries were used as conduits for these attacks. Scotland Yard had enough information to issue an arrest warrant and proceeded to make the arrest after data from the South Korean Atomic Research Institution was accessed. In all, over 150 intrusions were monitored at Rome Lab from 100 different points of origin. More than 100 other victims reportedly were hit.

Datastream Cowboy, a 16 year-old British student, pled guilty and was fined. His mentor, Kuji, a 22 year-old Israeli technician, was found not guilty because no laws in Israel applied to this incident.

Eligible Receiver (1997)

Eligible Receiver was the first Information Warfare (IW) exercise in this country. Thirty-five people participated on the Red Team over 90 days using off-the-shelf technology and software. The scenario was a rogue state rejecting direct military confrontation with the United States, while seeking to attack vulnerable U.S. information systems. Some of the goals of the rogue state were to conceal the identity of the attackers and to delay or deny any U.S. ability to respond militarily. A number of cyber attacks (all simulated) were made against power and communications networks in Oahu, Los Angeles, Colorado Springs, St. Louis, Chicago, Detroit, Washington, DC, Fayetteville, and Tampa.

Although reliable, unclassified results are hard to come by it is generally believed government and commercial sites were easily attacked and taken down. This exercise served as a wake-up call for many. Gen. Campbell, head of the Pentagon's Joint Task Force – Computer Network Defense, wrote Eligible Receiver "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure."[6] Then Pentagon spokesman Kenneth Bacon said, "Eligible Receiver was an important and revealing exercise that taught us that we must be better organized to deal with potential attacks against our computer systems and information infrastructure." Sen. John Kyl said in 1998:

> Well, [cyberterrorism is] surprisingly easy. It's hard to quantify that in words, but there have been some exercises run recently. One that's been in the media, called Eligible Receiver, demonstrated in real terms how vulnerable the transportation grid, the electricity grid, and others are to an attack by, literally, hackers – people using conventional equipment, no "spook" stuff in other words.[7]

---

[5]Closely related to hacking, it means using a computer or other device to trick a phone system. Typically, phreaking is used to make free calls or to have calls charged to a different account.

[6]IAnewsletter. Vol. 3, No. 4, p. 10.

[7]Interview on Cyberterrorism, U.S. Information Agency, November 1998.

Solar Sunrise (1998)

In February 1998, a number of Department of Defense networks were attacked using a well-known vulnerability in the Solaris (UNIX-based) computer system. The attackers: probed Defense Department servers to see if the vulnerability existed; exploited the vulnerability and entered the system; planted a program to gather data; and then returned later to collect that data.

Some of the initial probe activities appeared to originate from Harvard University and the United Arab Emirates (UAE), moving on to Pearl Harbor and a number of Air Force bases: Kirtland, Lackland, Andrews, Columbus, Gunter, and Tyndall. Later intrusion activities were monitored from the UAE, Utah State University, and a commercial Internet web site to some of the same Air Force bases. Further activity was monitored at dozens of other U.S. military sites and universities. International activity was monitored in Germany, France, Israel, UAE, and Taiwan. Over 500 computer systems were compromised, including military, commercial, and educational sites, by attackers using only moderately sophisticated tools.

In the end, two California High School students were arrested and pled guilty. Their mentor, an 18 year-old Israeli, was also arrested and indicted.

Although the Department of Defense called it "the most organized and systematic attack to date," many dismissed its seriousness because "the Justice Department claimed that no classified information was compromised."[8] And details of precisely what the hackers did are not publicly available.

Lessons some have drawn, however, are that Solar Sunrise confirmed the findings of Eligible Receiver: U.S. information systems are vulnerable. Additionally, others indicate that various legal issues remain unresolved (e.g., statutory restrictions and competing investigative needs and privacy concerns that hinder searches), there are no effective indications and warnings system in place, intrusion detection systems are insufficient, and there is too much government bureaucracy that hinders an effective and timely response.

U.S. Views and Efforts

How adequately is the United States prepared to deal with these kinds of cyber threats, as well as more serious threats to national security through cyberspace? This section summarizes how the United States now approaches these issues. Although it appears the government is now thinking about cyberwarfare issues more than in the past, and appears better organized, it is not clear whether a national consensus has formed or will form as to whether cyber threats constitute serious national security threats requiring a clear national security response.

---

[8]See [http://www.sans.org/newlook/resources/IDFAQ/solar_sunrise.htm].

Despite formal pronouncements (see below), it appears the government holds two major views on this subject. One view suggests that cyberthreats are primarily a national security problem in that major U.S. national interests and critical infrastructure are threatened. Historically, U.S. national military and diplomatic power has often been brought to bear to protect those interests. A case can also be made that cyberthreats to the United States similarly threaten U.S. national interests. Another view holds that cyberthreats should be handled primarily by civil or domestic authorities. A major concern here is over a strong military role within the borders of the United States (as opposed to outside the borders). In addition, a variety of privacy and civil liberties concerns also raise concern over a stronger military role. In the past, threats to the United States from abroad could mostly be countered abroad. But today we live in an age where geographic borders are easier to broach and do not even exist in cyberspace. This represents a new challenge to decisionmakers.

Executive Branch

Policy and Doctrine. Several forms of guidance help shape U.S. policy toward cyber attacks and cyberwarfare. The most recent White House report on National Security Strategy notes "we face threats to critical national infrastructures, which increasingly could take the form of a cyber-attack in addition to physical attack or sabotage, and could originate from terrorist or criminal groups, as well as hostile states."[9] These annual reports play a major guiding role within the Executive Branch national security bureaucracy.

The Department of Defense plays a key role in defending U.S. interests in cyberspace. Various Defense Department directives provide guidance and define terms such as Information Operations and Information Assurance (see section on Terms & Definitions). For instance, the Joint Doctrine for Information Operations (Joint Pub 3-13, October 9, 1998), represents a key document in defining how U.S. joint forces use cyberwarfare to support U.S. military strategy. But much of what the military does in cyberspace today is an outgrowth of traditional views and approaches toward ensuring information security or InfoSec.

The military has been further guided by Joint Vision 2010 (JV-2010), a broad long-term strategic concept for joint military strategy and planning purposes promulgated by the Joint Chiefs of Staff. JV-2010 embraced information superiority and technological advantages designed to transform traditional warfighting. Its successor, JV-2020 (released May 30, 2000), extends the conceptual template established by JV-2010 to guide the continuing transformation of U.S. military forces. Among other things, JV-2020 states:

> changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control.

---

[9]The White House. A National Security Strategy for a New Century. Dec. 1999.

Also, the Quadrennial Defense Review (QDR) stated that asymmetric forms of warfare, such as information warfare, will become increasingly prevalent in the world, adding:

> because of the prevalence of such capabilities in the hands of potential future adversaries and the likelihood that such adversaries would resort to such means in the face of overwhelming U.S. conventional dominance, U.S. forces must plan and prepare to fight and win major theater wars under such conditions.[10]

In addition, Presidential Decision Directive No. 63 (PDD-63) established in May 1998 a national goal to protect the nation's critical infrastructure[11] by the year 2003. PDD-63 further states that any disruptions to infrastructures "be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."[12] More recently, the White House National Plan for Information Systems Protection (Jan. 2000) seeks to further identify U.S. critical infrastructure vulnerabilities as part of a longer term effort to find solutions through government and private sector cooperation.

The Bush Administration has not yet articulated a policy toward cyberwarfare or cyberterrorism. Some key officials, however, have suggested that efforts are underway. In March 2001, Deputy Defense Secretary Wolfowitz testified before Congress that the United States must develop new strategies to defend against (among other things) cyberwarfare.[13] And just prior to President Bush's June 2001 visit to Europe, National Security Council Advisor Condoleeza Rice indicated the President would consult with European leaders on developing a new framework to deal with common threats, such as information warfare.[14] Also, the Bush FY2001 Defense Supplemental request included $50 million for classified Information Warfare programs.

Organization. CRS Report RL30153 (Critical Infrastructures: Background and Early Implementation of PDD-63) provides details of government organization for PDD-63. Among a number of things, PDD-63 established the position of National Coordinator for Security, Infrastructure Protection, and Counter-terrorism on the National Security Council staff. This person, currently Richard Clarke, chairs the Critical Infrastructure Coordination Group (CICG), which serves as "the primary

---

[10]Department of Defense. *Report of the Quadrennial Defense Review*. May 1997.

[11]Critical infrastructures are categorized as follows: information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production, and storage.

[12]For a comprehensive and detailed overview of PDD-63, see Jack Moteff, *Critical Infrastructures: Background & Early Implementation of PDD-63*, CRS Report RL 30153, updated regularly.

[13]Jim Garamone, "Wolfowitz Discusses DoD Goals During Testimony," *American Forces Information Service News Articles*, March 7, 2001.

[14]Condoleeza Rice, A Mission to Build on Common Challenges," *The Washington Times*, June 11, 2001, p. A15.

interagency working group for developing and implementing policy and for coordinating the federal government's own internal security measures." The CICG includes high-level agency representation (including the Sector Liaisons[15]), the National Economic Council, and all other relevant agencies. PDD-63 also established a National Information Assurance Council (NIAC) that includes private and local and state government representatives in the various sectors or infrastructures. PDD-63 called for a National Infrastructure Assurance Plan to provide an assessment of national needs in protecting the nation's infrastructure, as well as guidance in pursuing possible budgetary and legislative remedies. The Federal Bureau of Investigation (FBI) through the National Infrastructure Protection Center (NIPC) is given a lead role in serving as an early warning center for information system attacks. There is also an extensive federal structure for dealing with terrorism.[16]

The Department of Defense and other military agencies play key roles in protecting sensitive information and infrastructure. Much of the responsibility for dealing with cyber threat and response policies is now consolidated under the Assistant Secretary of Defense C^3I (Command, Control, Communications, & Intelligence).[17] On October 1, 2000, U.S. Space Command at Peterson Air Force Base, Colorado, assumed operational responsibility for the CNA (Computer Network Attack) mission for the Department of Defense. U.S. Space Command now takes the military lead in defending DoD networks, as well as offensive information operations as an element of defending U.S. systems. CNA operations may also include counterrorism and support of U.S. military forces deployed in crisis or conflict.[18]

The services and the various defense agencies also contribute in various ways to the challenge of cyberwarfare. For example, the Joint Task Force – Computer Network Defense (JTF–CND) operations center opened in Virginia in August 1999. It was designed to serve as the focal point for defense of DoD computer systems.[19] Until that time, the various services and agencies had been left largely to determine how best to improve network and system security. The JTF–CND began a process whereby common directives were established and recommended. The JTF–CND currently retains operational command for CND (Computer Network Defense) while U.S. Space Command is building a long-term, robust CND capability at Colorado Springs. In addition, some of the reserve forces, such as the Army Reserve, have created information operations centers trained and manned by so-called cyber-defense warriors.

---

[15]Each of the critical infrastructures identified in footnote 7 are represented by a lead federal agency. For example, the Department of Treasury has the lead in banking and finance.

[16]See [http://cns.miis.edu/research/cbw/response.htm].

[17]According to DoD Directive 5137.1, the Assistant Secretary is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for C^3I, information management (IM), information operations (IO), counter-intelligence (CI), and security countermeasures (SCM) matters, including warning, reconnaissance, and intelligence and intelligence-related activities conducted by the Department of Defense.

[18]News Release, Sep. 29, 2000: [http://www.spacecom.af.mil/usspace/rel15-00.htm].

[19]Information about the Center can be found in, IAnewsletter, Vol. 3, No. 4, pp. 10-15.

Current Legal Framework. In addition to the various U.S. laws guiding the conduct of warfare in general and U.S. government conduct in cyberspace, a key document was produced by the Department of Defense that examined the range of treaties and international law as they might pertain to the conduct of cyberwarfare.[20] This document is apparently playing an important role in guiding U.S. consideration of defensive and offensive operations in cyberspace. In essence, it makes several conclusions. First, it concludes there is little likelihood that the international community will soon generate a coherent body of information operations law. Second, it indicates there are no clear legal remedies or vehicles to address the type of information operations activities being considered by the United States. Third, and perhaps most relevant, the document recommends analyzing the various elements and circumstances of any particular planned operation or activity to determine how existing international legal principles are likely to apply.

Some have pointed out key legal issues that remain unresolved. These include, for example, the need for international agreements for expeditious pursuit of those violating the law, law enforcement needs in the conduct of electronic surveillance of those launching cyber attacks, possible legislation to encourage information sharing between the private sector and the government by protecting proprietary information and shielding sensitive information from FOIA (Freedom of Information Act) requests, and the establishment of clear and appropriate rules of engagement for cyber defense activities.[21] Some of these ideas are likely to generate controversy as national security interests are balanced against privacy concerns, for instance.

Recent Initiatives. In January 2000, President Clinton announced a 10-point, $2 billion program designed to protect government computers and networks from cyber attacks. The President proposed spending this money to increase funding for research and development in identifying and addressing vulnerabilities, detecting cyber attacks, developing intelligence and law enforcement activities, and creating capabilities to respond and recover from cyber attacks. The White House had wanted the program to go into effect by the close of 2000, and for it to be fully operational by mid-2003. The Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information held hearings in February 2000, but further action was not taken. Richard Clark (former National Security Council Coordinator for Security, Infrastructure Protection, and Counter-terrorism) had expressed frustration on several occasions that Congress has neither acted on this proposal, nor similar Administration proposals designed to strengthen and fund U.S. security in cyberspace over the past two years.

Congressional Response, Reaction, and Activities

For the most part, the Executive Branch has taken the initiative thus far regarding information security and cyberwarfare issues. Congress regularly supports funding for a wide range of activities that are designed to protect government

---

[20]Department of Defense. Office of the General Counsel. *An Assessment of International Legal Issues in Information Operations*. May 1999.

[21]IAnewsletter, Vol. 3, No. 1.

information systems and data. Much of this funding goes for programs that can be considered information assurance. These efforts are found in virtually every federal agency and are simply part of the normal responsibilities of government agencies. An accurate account of total annual funding for these efforts is not available.

Congress also regularly supports a broad range of national security programs that are in various ways related to information assurance and information operations. Many of these are found in the services, and throughout the various defense agencies. Although requested, the Defense Department could not provide CRS with a budget estimate for these programs. In perhaps large part, this is because there remains some lack of consensus as to what constitutes information operations or cyberwarfare activities within the Defense Department (even though a DoD definition exists). In addition, many of the tasks that might be considered information operations are part of what the military ordinarily does. Nonetheless, neither the Defense Department nor Congress has fully separated out these activities. This makes it difficult therefore to determine whether the overall funding is adequate or redundant, or even effective.

Some in Congress introduced relevant legislation this year. For instance, in March 2000, Rep. Jim Saxton introduced H.Con.Res. 282, which designates cyberterrorism an emerging national security threat. The bill calls for federal and private sector partnership, a revised legal framework for dealing with the problem, and a new federal study to assess the threat posed by cyberterrorists. The bill was referred to the House Judiciary (subcommittee on Crime) and Commerce (subcommittee on Telecommunications, Trade, and Consumer Protection) committees on March 15, 2000 where it remains. In April 2000, Sen. Orrin Hatch introduced S. 2448 (Internet Integrity and Critical Infrastructure Protection Act of 2000). It was referred to the Senate Judiciary Committee on April 13, 2000, where it remained until Oct. 5, 2000 when it was placed on the Senate Legislative Calendar.

Congress has expressed concern in other ways also. Rep. Stephen Horn, for instance, recently gave poor grades to the various Executive Branch agencies for efforts to strengthen and secure government networks.[22] Rep. Curt Weldon has charged the Administration with neglecting the problem of cyberterrorism and cyber threats to the United States.[23]

Selected Foreign Views and Activities

This section is not intended to be comprehensive, but rather illustrative of some of the major actors in the cyberwarfare arena. In general, some hold views comparable to the United States, including the UK, Germany, and NATO. France, however, may be an exception, because many observers have concluded that the

---

[22]See Horn Releases First-Ever Government-Wide Computer Security Evaluation. News Release. House Subcommittee on Government Management, Information, and Technology. Sep. 11, 2000. "Overall, the government earned an average grade of 'D-'. More than one-quarter of the 24 major federal agencies received a failing 'F'."

[23]Rep. Curt Weldon made these remarks in a Keynote address at the InfoWarCon 2000 Convention, September 12, 2000, Washington, DC.

French may see a legitimate role for economic cyberwarfare in the pursuit of national objectives. Russian rhetoric portrays cyberwarfare as an act of war for which any response, conventional or with weapons of mass destruction, is deemed justified. China sees cyberwarfare as a legitimate form of asymmetrical warfare and is preparing cadres of computer professionals for this task. These views re examined in more detail below.

Russia

Many Russians argue that the danger of cyberwarfare ranks second only to that of nuclear war. More than one senior Russian military officer has supported the notion that

> from a military point of view, the use of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not . . . considering the possible catastrophic use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.[24]

Other Russians see a military role for cyberwarfare activities, where the goal is for competing sides to gain and hold information advantages over the other. This is accomplished by using specific information technology capabilities to affect an adversary's information systems, decision making processes, command and control system, and even populace.[25] Some Russians believe that after conflict begins, "combat viruses and other information related weapons can be used as powerful force multipliers."

More recently, on September 12, 2000, Russian President Vladimir Putin adopted the Russian Information Security Doctrine, which had been approved earlier at the June 23 meeting of the Russian Security Council. The new doctrine ostensibly provides the government with an enhanced legal framework for dealing with computer crime and assuring security in cyberspace. In another sense, this represents a partial attempt by Russia to deal with cyber threats it too faces from foreign and domestic sources.

---

[24]V.I.Tsymbal, "Kontseptsiya 'Informatsionnoy voyny'", (Concept of Information Warfare), speech given at the Russian-U.S. conference on "Evolving post Cold War National Security Issues," Moscow 12-14 Sep., 1995 p 7. Cited in Col. Timothy Thomas, "Russian Views on Information-Based Warfare." Paper published in a special issue of *Airpower Journal*, July 1996.

[25]Lester W. Grau and Timothy L. Thomas. "A Russian View of Future War: Theory and Direction," *The Journal of Slavic Military Studies*. Issue 9.3 (Sept. 1996), pp. 501-518.

People's Republic of China (PRC)

China is moving aggressively toward incorporating cyberwarfare into its military lexicon, organization, training, and doctrine. In fact, if a Revolution in Military Affairs (RMA) is defined as a significant change in technology taken advantage of by comparable changes in military training, organization, and doctrine, then perhaps China of all nations is experiencing a true RMA in cyberspace. Moreover, China's warfare development has cause some U.S. military leaders to express concern. For instance, Gen. Eberhart, who heads U.S. Space Command, said the U.S. military is concerned about China's intentions and is worried about China's developing the means to carry out computer network attacks.[26]

The Chinese concept of cyberwarfare incorporates unique Chinese views of warfare based around the People's War concept (modern) and the 36 Strategems (ancient). Both are indigenous views of how to wage war at the strategic, operational, and tactical level. China also is heavily influenced by Marxist-Leninist ideology regarding warfare. Much of its approach has to do with an emphasis on deception, knowledge-style war, and seeking asymmetrical advantages over an adversary. Cyberwarfare is seen as a "transformation from the mechanized warfare of the industrial age to . . . a war of decisions and control, a war of knowledge, and a war of intellect."[27]

China is pursuing the concept of a Net Force (battalion size), which would consist of a strong reserve force of computer experts trained at a number of universities, academies, and training centers. Several large annual training exercises have already taken place since 1997. The Chinese have placed significant emphasis on training younger persons for these tasks.

United Kingdom (UK)

The UK view toward cyberwarfare is similar to that of the United States. Basically, it notes that information warfare refers to actions affecting others' information systems while defending one's own systems in support of national objectives.[28] Furthermore, the UK uses a legal framework based around a number of existing laws it believes largely can be applied to cyberspace activities.[29] This

---

[26]"U.S. Military Concerned about China's Cyberwarfare Capabilities: General," *Agence France Presse*, March 28, 2001.

[27]Military Strategic Research Center, Beijing, May 1996.

[28]In June 2000, the UK defined IW as "integrated actions undertaken to influence decision makers in support of political and military objectives by affecting others information, information based processes, C2 [command & control], systems, and CIS [critical infrastructure systems] while exploiting and protecting one's own information and/or information systems."

[29]These include the: Computer Misuse Act (1990), Telecommunications Act (1984). Telecommunications (Fraud) Act 1987, Obscene Publications Act (1959 and 1964), Protection of Children Act (1978), Criminal Justice Act (1988), Criminal Justice and Public

(continued...)

suggests that the UK views cyberattacks against individuals and corporations as civil and criminal issues that can be handled accordingly. More recently, the Regulation of Investigatory Powers Act 2000 (RIP), would allow the UK government to intercept and read e-mail, and require decryption of personal files on demand. The UK government says RIP puts "intrusive investigative techniques on a statutory footing for the very first time; provides new powers to help combat the threat posed by rising criminal use of strong encryption; and ensures that there is independent oversight of the powers in the Act."[30]

Germany

For the most part, the German perspective toward cyberwarfare is comparable to that of the United States and the UK.[31] It recognizes a legitimate role for offensive and defensive information warfare in pursuit of national objectives. Germany tends to be somewhat more systematic than the United States, however. For purposes of thinking about cyber threats and cyber responses, nation states are considered separately from non-state actors (such as political activists, international organizations, and the media), criminals (organized crime, hackers, etc.), and individual actors (including religious fanatics and special forces).

In two ways, however, German views toward information warfare may differ. Germany may include management of the media as an element of information warfare. In addition, Germany may be weighing a rationale for economic cyberwarfare similar to the French (see below). This may be due to several reasons: Germany has assessed the potential for economic damage that can be done to German business and economy; Germany may have experienced significant economic losses to France over a case involving industrial espionage in cyberspace; and Germany may be seeking ways to mitigate the consequences of potential cyber attacks.

North Atlantic Treaty Organization (NATO)

Reportedly, there is a classified NATO definition of information warfare, but it is not publicly available. The development of such a definition is noteworthy given that at a NATO conference in early 2000, 17 different descriptions or definitions of IW were being used by the individual delegate countries. Generally, however, the NATO definition is believed to be compatible with the U.S. perspective.

---

[29](...continued)
Order Act (1994), Data Protection Acts (1984 and 1998), Theft Acts (1968 and 1978), Forgery and Counterfeiting Act (1981), Copyright Design and Patents Act (1988), and Interception of Communications Act (1985).

[30][http://www.homeoffice.gov.uk/ripa/ripact.htm].

[31]The German section is taken largely from a paper presented by Andy Jones, The European Perspective, at the InfoWarCon 2000 Convention, September 11, 2000, Washington, DC. Much of his analysis was taken from French and German language Web sites.

France

The French apparently view cyberwarfare as having two main elements: military and economic (or civil).[32] The military concept envisions a somewhat limited role for cyberwarfare activities. Their military concept sees cyberwarfare activities taking place largely in the context of low intensity conflict or operations other than war, undertaken generally within the framework of NATO and the United Nations (and often under the control of the United States). In this context, allies are not considered adversaries.

In contrast, the economic or civil concept includes a wider range of potential cyberwarfare applications. The French view seems to assume a much broader and deeper basis for conflict in the economic sphere; economic peace does not exist as much as an environment in which competitors pursue zero-sum market advantages. The French do not see themselves bound by NATO, UN, or U.S. approval. Their perspective toward economic conflict allows for one to be both an ally and an adversary at the same time. The French even have an economic school for information warfare.[33]

France may also have a different perspective toward monitoring its citizens in cyberspace. Reports have surfaced that the French have their own version of Echelon (reportedly a U.S. effort – not officially verified – aimed at intercepting virtually all private global communications).[34] Frenchelon, as some have called it, reportedly is used to monitor and analyze French communications, especially in the Paris region.[35]

Non-State Actors

There is considerable evidence that some non-state actors and anti-government forces use cyberspace as another tool to wage their fight against various nations. For example, Mexico's Zapitista movement uses the World Wide Web to elicit support for its cause ([http://www.ezln.org]). Afghanistan's Taliban militia – a movement that controls most of Afghanistan – maintains a site with a range of material and even solicits contributions from abroad. Similarly, there is an Internet site Basque National Liberation Movement (a separatist movement in the region between Spain and France.

Cyberterrorism

There appears to be reasonable evidence available that terrorist organizations use cyberspace to conduct the business of terrorism. Terrorists use the Internet and the

---

[32]See [http://www.infoguerre.com] (in French).

[33]See [http://www.ege.eslsca.fr] (in French).

[34]See Richard Best. *Project Echelon: U.S. Electronic Surveillance Efforts*. CRS Report RS204444, Mar. 2, 2000.

[35]"Frenchelon, the Large Ears Made in France." See [http://www.zdnet.fr/actu/tech/secu/a0014768.html].

World Wide Web to communicate with each other, recruit members, gather intelligence, raise money legally and illegally, organize and coordinate activities, obtain illegal passports and visas, and distribute propaganda. For instance:

- Some Afghan-based terrorists, such as Osama bin-Laden, reportedly have computers, communications equipment, and large data storage disks for their operations.[36]
- Hamas, a Middle Eastern terrorist organization, reportedly uses Internet chat rooms and e-mail to plan and coordinate operations in Gaza, the West Bank, and Lebanon.[37]
- Hizballah, another Middle Eastern group, manages several Internet Web sites for propaganda purposes ([http://www.hizbollah.org/]), to describe attacks against Israel ([http://www.moqawama.org/]), and one for news and information ([http://www.almanar.com.lb/]).
- Government computers reportedly were crashed by terrorist groups during elections in Indonesia, Sri Lanka, and Mexico.
- Irish Republican Army (IRA) supporters reportedly leaked sensitive details on British army bases in Northern Ireland on the Internet. Sinn Fein also maintains a web site ([http://sinnfein.ie/]).

But is this cyberterrorism? If terrorism is defined as an act of violence designed to achieve political objectives, do these activities constitute acts of violence? Should these types of activities more accurately be described as techno-terrorism, the terrorist's use of technology, satellite communications, e-mail, and the Internet in their business? Some observers express concern that terrorists want to bring down the Internet. But if terrorists rely on the Internet, why would they want to bring it down? Others, in and out of government, express concern about terrorists targeting power and communications grids, for example. But Richard Clarke (National Security Council Coordinator for Security, Infrastructure Protection, and Counter-terrorism), has said several times it does not appear that terrorist groups actually are planning to use the Internet for these kinds of activities.

So is cyberspace another tool to be exploited by terrorists, and does U.S. and western reliance on information systems and cyberspace represent a significant vulnerability awaiting terrorist attack? Currently, there does not appear to be a consensus answer, although most would agree that attention and resources should be devoted to this issue given the high stakes.

Challenges and Issues for Congress

Cyberwarfare is an emerging issue of national interest. At this point, however, a coherent consensus strategy is lacking. Should cyber threats be considered primarily

---

[36]Afghanistan, Saudi Arabia,: Editor's Journey to Meet Bin-Laden Described," *London al-Quds al-'Arabi*, FBIS-TOT-97-003-L. Nov. 27, 1996, p. 4.

[37]Israel: U.S. Hamas Activists Use Internet to Send Attack Threats," *Tel Aviv IDF Radio*, FBIS-TOT-97-001-L, Oct. 13, 1996.

a domestic or civil responsibility for law enforcement and the judicial system, or are cyber threats to U.S infrastructure a national security responsibility? In the past, responsibilities were more easily managed because geography often represented obstacles to adversaries. Geography is much less an obstacle today.

Another reason a coherent consensus approach may be lacking is due to the complexity and diversity of the topic and the absence of technological means to determine unambiguously and in real time where computer or network attacks are coming from. Without an extensive commitment of time and resources, cyber attacks are difficult to trace with a high degree of confidence.

But without clear national guidance, issues such as appropriate organization, responsibility, and funding will likely remain problematic. In light of the fact that the U.S. response to information capabilities is still evolving, Congress may seek to determine the scope of executive branch spending for cyberwarfare-related activities, and further examine whether such levels are sufficient, coordinated, or duplicative. The government's conceptual and organizational approach toward cyberwarfare may be of legislative interest. Congress may also weigh in on whether an individual or some agency should have primacy in issues dealing with cyberwarfare.

Appendix: Terms & Definitions

For ease of discussion, **cyberwarfare** in this report is used broadly to mean warfare waged in cyberspace. It can include *defending* information and computer networks, *deterring* information attacks, as well as *denying* an adversary's ability to do the same. It can include *offensive* information operations mounted against an adversary, or even *dominating* information on the battlefield. Other, more technical and precise terms are indicated below for reference.

Information Warfare (IW) "involves actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks." (Department of Defense Directive 3600.1) IW is further defined as Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." (IATAC TR-97-002).

Note that some key observers outside of government have defined IW to include personal and corporate warfare (attacks on individuals or companies by other individuals or companies).[38] Some Europeans tend to share this perspective as well. Critics charge that "warfare" is not focused on individuals or commercial organizations. They argue that attacks against individuals are civil or criminal litigation issues, while attacks against corporations by other companies are acts of

---

[38]See Winn Schwartau, *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*. New York, NE: Thunder's Mouth Press, 1994, pp. 473-587.

industrial espionage, although they acknowledge that an attack by a government or terrorist group may in fact be Information Warfare.

Special Information Operations (SIO) are information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to national security of the United States, require a special review and approval process. (Department of Defense Directive 3600.1)

Information Superiority is "that degree of dominance in the information domain which permits the conduct of operations without effective opposition." (Department of Defense Directive 3600.1). It is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information Assurance (IA) is "Information Operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities." (Department of Defense Directive 3600.1)

- **IA Authentication** are security measures "designed to establish the validity of a transmission, message, or originator, or a mean[s] of verifying an individual's authorization to receive specific categories of information." (National Telecommunications Information Systems Security Instructions – NSTISSI – 4009).
- **IA Availability** refers to timely, reliable access to data and information services for authorized users. (NSTISSI – 4009)
- **IA Confidentiality** is assurance that information is not disclosed to unauthorized persons, processes, or devices. (NSTISSI – 4009)
- **IA Integrity** is protection against unauthorized modification or destruction of information. (NSTISSI – 4009)
- **IA Nonrepudiation** is assurance that the end user of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can subsequently deny having processed the data. (NSTISSI – 4009)

Computer Network Attack (CNA) are operations designed to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers or networks themselves. (Department of Defense Directive 3600.1)

Electronic Warfare (EW) is defined as "any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack an enemy." (Chairman, Joint Chiefs of Staff MOP 6). It is a well-established component of contemporary combat not necessarily involved with cyberspace. For a highly useful discussion of EW and other issues, see CRS Report RL30639 (Electronic Warfare: EA-6B Aircraft Modernization and Related Issues for Congress).